Centre for Information Policy Leadership
Hunton Andrews Kurth

31 May 2019

**Comments by the Centre for Information Policy Leadership on the UK Information Commissioner's Draft Code of Practice for Age Appropriate Design for Online Services**

On 15 April 2019, the UK Information Commissioner's Office (ICO) issued its Draft Code of Practice for Age Appropriate Design for Online Services (Draft Code or Code).[1] The ICO invited public comments on this document by 31 May 2019.

The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit the comments and recommendations below as input for the ICO's final Code (Final Code).

## Comments

CIPL welcomes the ICO's initiative to provide guidance about how to appropriately safeguard children's personal data when providing online services, as this has not previously been explored in detail.

CIPL recognises the importance of the issues addressed in the Draft Code and that there will be many benefits for individuals and for information society service providers in the development of clear and vigorous standards for online services for children.

In this brief response, CIPL has sought to point to some key and strategic areas for consideration relevant to the overall structure and direction of the Code. CIPL realises the real time and political pressure for the ICO to deliver on the requirements of the UK Data Protection Act 2018 (the UK DPA) and to present this Code to the UK Parliament. Yet, the impact of the Code on so many organisations and, ultimately, on the use of online services and products by children, as well as the impact and scope of the Code on design related issues, require serious and deep consideration, consultation and even co-opting of solutions from user design and industry experts. CIPL believes that the Final Code and the actual process of coming up with design related guidance would benefit from such further engagement. CIPL would be willing to work with the ICO to facilitate this type of deeper discussion with relevant CIPL members and experts from the user design community.

---

[1] Age appropriate design: a code of practice for online services, available at https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 75 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

CIPL believes that to protect children effectively, the Final Code must be robust in practice while also enabling a workable online environment. In this context, CIPL believes that the Draft Code may be sometimes too far reaching and that its practical implementation may trigger unintended consequences. However, CIPL believes that, working with industry, these challenges are not insurmountable, and CIPL sets out various suggestions to make the Code more practical from the standpoint of implementation.

In particular, CIPL believes that the Draft Code does not sufficiently take into account the following points:

- The Code should **not extend to cover services** that are not offered to or intended for children, and which children are not likely to access.

- **The Code should reflect the risk-based approach** enshrined in the GDPR.[3] CIPL believes it important to acknowledge that not all processing of personal data relating to children raises the same levels of risk. Article 5 of the GDPR includes the overarching principles relating to the processing of personal data. Among them are the principles of fairness, transparency and accountability. In determining what is required to achieve compliance with these overarching principles, regard should be had to the particular risk in order to determine a proportionate approach and specific compliance steps.

- The Code should recognise the need to implement **age verification** mechanisms only when the service is directed to children.

- The Code should recognise the **developing autonomy of young people** and avoid imposing requirements that have the effect of treating older teenagers as children.

- The Code should provide a **flexible and adaptable** set of requirements in relation to the provision of privacy disclosures depending on the age category of the children.

- The Code should further consider the **benefits linked to geolocalisation and personalisation** of content in the context of online services likely to be accessed by children.

- The Code should be **legally robust** and not exceed the ICO's statutory mandate in order to avoid possible legal challenges in the future.

- The Code should clarify the **role of data protection impact assessments (DPIAs)** in the context of processing personal data for the provision of online services likely to be

[3] See CIPL paper on Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

accessed by children by integrating proportionality considerations and limiting the impact assessment to the privacy of individuals and their related rights and freedoms.

In sum, CIPL believes that the Code would benefit from further constructive engagement with industry to ensure a robust and proportionate approach, which can be implemented to the benefit of individuals and information society service providers.

## 1. Practical Application of the Code

### A. Which Services are Covered?

CIPL recognises that Section 123(1) of the UK DPA requires that the Commissioner prepare a code of practice that provides guidance on standards of age-appropriate design of relevant information society services which are likely to be accessed by children[4] (emphasis added).

The question of how such likelihood is determined under the UK data protection regime has been considered in case law under the 1998 Act, albeit in another context, in the case of *R (Lord) v Secretary of State for the Home Department*.[5] In that case, the Court considered whether the provision of subject access would be likely to prejudice the prevention or detection of crime. The Court had to determine whether it was likely that the identified prejudice would result. The judge said the test of likelihood requires:

> "a degree of probability where there is a very significant and weighty chance of prejudice to the identified public interests".

The ICO's guidance on this[6] stated:

> "This test recognises that a data controller should only apply the exemptions when it is necessary to do so in order to safeguard the relevant purposes. It sets a higher bar than being merely 'possible', and requires a data controller to establish a strong link between the data processing and its prejudicial effect.
>
> Example
>
> An insurance company is concerned about the validity of a claim and conducts a standard investigation into whether it is an attempted fraud. While the claim is still being assessed, the customer makes a subject access request for the information held about them. The company refuses to provide any information, saying that it would prejudice an ongoing attempt to detect a criminal act. A basic assertion that releasing

[4] See Section 123(1) of the UK Data Protection Act 2018, available at https://www.legislation.gov.uk/ukpga/2018/12/section/123.
[5] *R (Lord) v Secretary of State for the Home Department* [2003] EWHC 2073, Justice Munby at Paragraph 100.
[6] UK ICO Guidance, Using the Crime and Taxation Exemptions, Data Protection Act, 2015, available at https://ico.org.uk/media/for-organisations/documents/1594/section-29.pdf.

the information might prejudice this and future investigations is not sufficient to rely on the exemption. The company would need to demonstrate more precisely how providing the information in this case would adversely affect their ability to investigate and prevent criminally fraudulent claims".[7]

CIPL notes that the Code appears to have reversed the burden of proof and requires controllers to prove that they are not covered by the Code, suggesting that they must be able to evidence that their services are not likely to be accessed in practice by children.[8] CIPL is concerned that this reverses the usual burden of proof and would place practical constraints on sites and services that are not offered to or intended for children, and which children are not likely to access.

**B. Risk Assessment**

Even where services are likely to be accessed by children and young people, CIPL is concerned that the Code has adopted an approach that would have the effect of treating all individuals under the age of 18 uniformly as children. Although Section 123(4)(b) of the UK DPA requires the Commissioner to have regard to the United Nations Convention on the Rights of the Child (UNCRC), it does not mandate that the ICO adopt its definition of a child.

Article 8 of the GDPR requires verifiable parental consent for the processing of data of children under 16 and gives Member States the ability to lower that age to 13. This approach, practically speaking, sets the age of presumed digital literacy between 13 and 16, depending on the age threshold selection of Member States. It reflects a common European view of the capacity of children and young people who have grown up with technology and whose educations have included digital literacy.

In this context, CIPL believes that:

- The GDPR criteria for parental consent more accurately reflect the maturity of children and young people in the digital space; and

- From a practical perspective, it would be far more workable for the Code to work with and reflect the standards contained in the GDPR.

Finally, CIPL is concerned that the Draft Code insufficiently acknowledges the developing personal autonomy of young people. CIPL would point out that a young person is regarded as

[7] *Id*. at page 6.

[8] *Supra* note 1 at page 15, "you must be able to point to specific documented evidence to demonstrate that children are not likely to access the service in practice".

competent to decide whether he or she is able to consent to medical treatment at the age of 16 years and may be able to do so at an earlier age if she is "Gillick competent".[9]

### C. Age – Stages of Development

CIPL notes that the Draft Code sets out five separate categories of ages.[10] This is important and useful material which may be valuable in the design of services directed towards children of different ages.

CIPL welcomes this research and the guidance provided. However, CIPL is concerned that this may result in a rigid set of requirements in relation to the provision of privacy information under Chapter 3 of the Draft Code.

It is CIPL's view that:

- Elements of the material do not fall within the data protection regime (e.g. the provision of educational resources for parents[11] or within the context of age-appropriate information relating to parental controls, information to parents about the UNCRC[12]);

- The material appears overly prescriptive (e.g. to provide "full information in a format suitable for parents to sit alongside the child focused information" for sites aimed at individuals between 16-17 years of age[13]); and

- The material appears too detailed in terms of the number of different categories of notice and tools that would need to be implemented and will be both confusing for users and impossibly unwieldy for service providers. For example, a single service, providing a uniform experience to all users, may end up having multiple privacy notices and legal documents for that service in order to accommodate the different age categories of its potential users. This could end up confusing users with an overload of information and require them to navigate through different documents to find the notice most relevant to them which may in turn damage users' overall service experience.

---

[9] Gillick competence is used in medical law to decide whether a child (under 16 years of age) is able to consent to his or her own medical treatment, without the need for parental permission or knowledge. It is based on the House of Lords decision in *Gillick v West Norfolk and Wisbech Area Health Authority* [1985] UKHL 7.

[10] *Supra* note 1 at pages 32 and 98.

[11] *Id*. at page 33, "Provide resources for parents to use with their children to explain privacy concepts and risks within your service. Provide resources for parents to use with their children to explain the basics of your service and how it works, what they can expect from you and what you expect from them".

[12] *Id*. at page 58, "You should also provide parents with information about the child's right to privacy under the UNCRC…"

[13] *Supra* note 1 at page 34.

Organisations should have flexibility to implement one single notice and set of tools that are understandable for a wider audience, and complement that with specific resources for parents and children to support age-specific or special capacity needs.

### D. Age Verification

CIPL is aware of the many debates around the development and use of age verification measures. CIPL reiterates its view that requiring all users to verify their age before being able to access some services or adjusting their privacy settings would result, in many cases, in a degraded user experience or barriers to entry to the site and the inappropriate and disproportionate collection of personal data (including processing of intrusive data, perhaps involving government IDs or other methods of identification). This will especially be the case for services that are not targeted to children.

The Article 29 Working Party guidelines on consent[14] expressly refer to age verification and state "[w]hen providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities". The approach of the Code should be consistent with that guidance and only require age verification when the services are directed to children below the age of consent.

Additionally, age verification mechanisms should not lead to excessive data processing. Collecting individuals' ID cards or Passports would be a disproportionate approach. While it may be appropriate to collect more information for age verification if the contemplated processing includes certain high risk activities, for general use cases, the collection of information for age verification should take place consistent with the GDPR principle of proportionality. CIPL believes it is important to support the use of age verification mechanisms such as neutral age screening, which appropriately balances the interest in confirming age with other data protection rights of individuals.

### E. Geolocation

A number of CIPL members have raised specific concerns at the prospect of geolocation options being turned off by default.[15] There are concerns that this could cause significant impact on regional or location-based services or in situations where there are contractual or IP limitations with respect to the geographies where certain content can be offered. In this case, users will not be able to access the content unless they manually update their privacy preferences to allow for geolocation data to be collected. One approach to address this could be to define geolocation to exclude information such as city or country, which is often all that is needed to access content, and which cannot be used to identify an individual.

---

[14] Article 29 Working Party Guidelines on Consent under the GDPR as last revised and adopted on 10 April 2018, available at https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030 at page 25.
[15] *Supra* note 1 at page 54.

Furthermore, geolocation can also be used as a child safety mechanism and there is a concern that such a beneficial and potentially life-saving use of geolocation data will be hindered if turned off by default.

The use of location information for certain services is expected by users and sometimes necessary to ensure the full functionality of the service or even protect individuals' interests. For example, if a user searches for a hospital in an emergency situation they expect to get quick results for hospitals in their city, and that would also protect users the most by enabling them to get help quickly.

### F. Personalisation of Services

The Draft Code aims to integrate a standard whereby settings related to personalisation of services should be turned off by default. However, many personalisation services operate to improve the user experience. For example, personalised recommendations of books or films or video on demand (VOD) services, which provide users with content consistent with their interests. In online gaming, personalisation services enable users to resume the game where they left off and to claim in-game earned rewards.

In the case of VOD services, turning personalisation off by default may actually drive users away from well regulated VOD platforms that already comply with the OFCOM broadcasting code and advertising codes such as the BCAP and CAP codes.

In addition, personalised content can help prevent age-inappropriate content from being suggested to users. CIPL believes it is the abuse or misuse of personalised services which should be addressed, not the services themselves.

## 2. Legal Analysis

CIPL is strongly supportive of the use of codes together with other compliance tools which help deliver accountability for controllers and processors and understanding for individuals.

CIPL recognises the aim of the ICO to use the Code as an opportunity to produce compendious guidance on issues associated with children's personal data. However, this approach may jeopardise the Code on the one hand and confuse users on the other.

### A. Scope of the Draft Code

CIPL is concerned that the scope of the Draft Code may exceed the ICO's statutory mandate and this puts the Code at risk of criticism and potential legal challenge.

Under the GDPR, supervisory authorities are not empowered to create codes of practice that have legal effect. The structure and nature of GDPR codes of conduct under Articles 40 and 41 of the Regulation differ from the UK concept of Commissioner's codes of practice. The Final

Code will be made under Section 123 of the UK DPA. While the ICO can issue guidance associated with a statutory code, it does not appear that it can extend the remit of the statutory code. In fact, the UK DPA does not seem to include a general power for the ICO to prepare and issue codes of practice admissible in legal proceedings which cover issues that are outside of the specific area of age appropriate design. CIPL believes that the current Draft Code conflates the specific topic of the Code (age appropriate design) with the wider topic of the online protection of children and general compliance with the GDPR.

An example of this can be seen on page 7 of the Draft Code:

> "In particular this code sets out practical measures and safeguards to ensure processing under the GDPR can be considered 'fair' in the context of online risks to children…"

The section goes on to list fourteen specific Articles of the GDPR. The purported extension of the Code to address online risks to children, generally, and the wide scope of GDPR elements which it purports to cover, indicate that the scope of the Code may be considered to exceed the Commissioner's powers. It runs the risk that once final and implemented by industry, the Code could be challenged on this basis (see further discussion under point C below on the relationship between the Code and GDPR processing of children's data).

CIPL also notes that there is no elaboration on what is covered by the term "age appropriate design" in the Draft Code. Section 123(7) of the DPA states that it means the "design of services so that they are appropriate for use by, and meet the development needs of, children".

Therefore, CIPL recommends prefacing the Final Code with a clear statement that the Code provides guidance on the area of age appropriate design only and does not apply to areas outside of this, including, for example, online content which is regulated through other codes by other regulators in the UK (see discussion below on relationship between the Code and other regulatory regimes).

### B. Nature of Codes of Practice

The role of a code of practice under Section 123 of the UK DPA is to provide guidance on standards of age appropriate design. The obligation to design services falls on the relevant controller, not the Commissioner. This is a different approach to that taken in respect of codes under Article 40 of the GDPR which covers codes of conduct. Under Article 40, a code of conduct agreed by bodies representing categories of controllers will operate for the purpose of "specifying the application of this regulation" with regard to the listed matters, including fair and transparent processing, the exercise of individuals' rights and other detailed matters.

There is a difference between a code that provides guidance to a wide range of controllers, as the Commissioner's Draft Code is meant to do, and one which specifies particular methods of compliance with the GDPR, as the industry codes envisaged under Article 40 of the GDPR are intended to do. CIPL is concerned that the Draft Code has adopted an approach of seeking to

particularise and specify compliance matters in a too detailed and prescriptive manner. CIPL believes that this may make it difficult for controllers to comply and might impede the development of more flexible services.

### C. Relationship Between the Code and GDPR Processing of Children's Data

As drafted, the Code has an extensive scope. It not only covers areas relating to the design of information society services directed to and likely to be accessed by children, but also includes further interpretation and guidance on the processing of personal data generally, as covered by the GDPR. This guidance from the ICO is certainly important and helpful to controllers and processors that process children's data. However, such further guidance distracts from the real scope and nature of the Code, and from its legal standing – to provide additional and more specific design-related guidance and steer for affected organisations. CIPL does not believe that the Final Code should address matters and obligations already envisaged by the GDPR. Rather, such guidance should be the subject of parallel stand-alone guidelines on the processing of children's data under the GDPR. Such guidance should be published at the same time as the Final Code or within a reasonable time afterwards but would be clearly different from the Code in terms of legal status and subject matter.

### D. Relationship Between the Code and Other Regulatory Regimes

CIPL recognises that the ICO wishes to cover a wide scope and also acknowledges that the boundaries of what is within and outside a code of this nature may be somewhat hazy in places. However, in some areas, it is CIPL's view that the Draft Code appears to move into areas which are subject to separate legislative regimes and runs the risk of creating confusion as to which regulatory provisions apply. CIPL notes, for instance, that the Code makes specific reference to the Committee of Advertising Practice (CAP)[16] guidance, which relates to advertising restrictions not regulated by the ICO, but it is not clear why this is referenced in a data protection code.

CIPL suggests clarifying Sections 4 and 5 of the Code. The Code should focus only on data processing activities and not interpose other standards that are overseen and enforced by other regulators. Codes designed to regulate online content and the audio-visual industry more generally, and outside of the sphere of data protection, already exist, including the OFCOM broadcasting code and the Advertising Standards Authority advertising codes. Such codes already provide for robust enforcement with backstop powers and clear guidance on protecting children from harmful content or inappropriate advertising. As such, the ICO's Final Code should not seek to regulate such areas outside of data protection.

### E. Data Protection Impact Assessment (DPIA)

DPIAs are specific legal tools introduced under the GDPR. Article 35 requires the use of a DPIA where processing is likely to result in a high risk to the rights and freedoms of natural persons,

[16] *Supra* note 1 at page 37.

in particular where new technologies are used. Under Article 35(4), supervisory authorities must establish and make public a list of the kinds of processing operations which are subject to the requirement of a DPIA and communicate the list to the Board. Under Article 35(6), a supervisory authority must go through the consistency mechanism where such lists involve the offering of goods and services to individuals or the monitoring of their behaviour in several Member States or may substantially affect the free movement of personal data within the Union.

The Draft Code purports to[17]:

- Make the use of a DPIA mandatory in every case of processing where children are likely to access a service;
- Instruct the controller to take into account specific issues of age, capability and development;
- Instruct the controller to take account of a list of potential detriments including ones wholly unrelated to the privacy interests and rights and freedoms of children; and
- Instruct the controller to "build in compliance" with the Code as part of the DPIA outcome.

CIPL believes this raises a number of procedural and legal questions:

- In purporting to make a DPIA mandatory in these cases the Commissioner is effectively exercising the Article 35(4) power. The Board has published a list of the topics that may merit a mandatory DPIA which includes personal data related to vulnerable groups. As such, it appears that under Article 35(6), the adoption of a requirement to conduct a DPIA in every case involving the processing of personal data relating to children, must be subject to the consistency mechanism. It would be helpful to controllers operating in multiple Member States for the Code to provide a clear explanation of the relationship between the mandatory DPIA and Article 35(6).

- Although CIPL does not dispute that children merit special protections with respect to how their data is processed, the imposition of the requirement to conduct a DPIA for every processing, irrespective of the vulnerability or risk involved in the processing, and the mandatory inclusion of specific issues to consider does not sufficiently take into account the risk-based and proportional approach set out in Article 35(7) of the GDPR. A DPIA should only be required for high risk processing activities.

- A DPIA is intended to address the protection of personal data and the necessity and proportionality of processing operations in relation to the purposes of the processing. Specifically, Article 35(7)(d) of the GDPR refers to security measures and "mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and

[17] *Id*. at pages 82-88.

other persons concerned". Recital 91 gives some interpretative advice as to the nature of the risks to rights and freedoms which will be relevant, such as processing which would prevent individuals from exercising their rights. However, the list of potential detriments which the Draft Code sets out include matters which are outside the scope of a DPIA, being wholly unconnected to the privacy of individuals or their related rights and freedoms. For example undermining parental authority, interrupted or inadequate sleep patterns or encouraging risk-taking behaviours.[18] These matters may legitimately be included in a code on online harms rather than in a data protection code.

- Most concerning to CIPL is the purported requirement that the DPIA must ensure compliance with the Code and the threat that a failure to do so will result in enforcement action. This has the effect of elevating the status of the Code to a set of mandatory legal obligations equivalent to those in the GDPR itself.

### F. Relationship with United Nations Convention on the Rights of the Child (UNCRC)[19]

The first standard of the Draft Code states that the best interests of the child should be the primary consideration when an information society service provider designs and develops online services likely to be accessed by a child.[20] The Code relies on Article 3 of the UNCRC in formulating this standard.

Firstly, as CIPL previously noted, it would be helpful to clarify that the Code does not apply to designers or developers that are not controllers.

Secondly, CIPL is concerned that the first standard of the Code does not accurately reflect the mandate of the UK DPA. Section 123(4) of the UK DPA states that, in preparing the Code, the Commissioner must have regard to the UK's obligations under the UNCRC. This means that the ICO must consider the UK's obligations to seek to ensure the rights of children in preparing the Code. However, as currently drafted, the Code appears to conflate the ICO's obligation with the obligations of service providers themselves.

This is apparent on pages 17 and 18 of the Code which state, "[a]lthough as a provider of online services you may not be directly subject to the UNCRC, Article 5(1)(a) of the GDPR says personal data shall be processed lawfully, fairly and in a transparent manner". Relying on Recital 38 of the GDPR, which holds that children merit specific protection with regard to their personal data, the Draft Code further notes, "[i]f you consider the best interests of child users in all aspects of your design of online services, then you should be well placed to comply with the 'lawful, fairness and transparency' principle and take proper account of Recital 38. The principle of the 'best interests of the child' is therefore both something that you specifically need to consider when designing your online service and a theme that runs throughout the provisions

[18] *Supra* note 1 at page 87.
[19] 1989 United Nations Convention on the Rights of the Child.
[20] *Supra* note 1 at page 5.

of this code". In other words, the Code, as currently drafted, shifts the ICO's obligation to consider the UK's obligations under the UNCRC in preparing the Code to service providers to consider in the design of their online services.

CIPL is concerned that this gives the impression that the online service provider has a direct duty to consider the best interests of the child user and promote and support children's rights. The UNCRC does not place such an obligation on controllers. The Commissioner has a legal obligation in framing the guidance to consider the best interests of the child and to develop and draft guidance so as to support that, but that obligation is not transferred to the provider of the online service.

Finally, in considering the UK's obligations under the UNCRC in preparing the Code, the UK should only issue guidance with respect to the best interests of the child as it relates to data collection and the protection of privacy only and not with respect to the best interests of the child as it relates to all online behaviour which would be outside the remit of the ICO's regulatory scope.

## Conclusion

CIPL is grateful for the opportunity to comment on the ICO's Draft Code of Practice for Age Appropriate Design for Online Services and hopes the above will prove useful to the ICO as it works on the Final Code.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, [redacted] Markus Heyder, [redacted] Nathalie Laneret, [redacted] or Sam Grogan, [redacted]